

**GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE INSPECTOR GENERAL**

**AUDIT OF THE USE OF UNAUTHORIZED
SOFTWARE AT THE
OFFICE OF CONTRACTING AND PROCUREMENT**



CHARLES C. MADDOX, ESQ.
Inspector General

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Inspector General

Inspector General



February 27, 2002

Jacques Abadie
Director
Office of Contracting and Procurement
One Judiciary Square
441 Fourth Street, N.W., Suite 800
Washington, D.C. 20001

Suzanne J. Peck
Chief Technology Officer
Office of the Chief Technology Officer
441 Fourth Street, N.W., Suite 930S
Washington, D.C. 20001

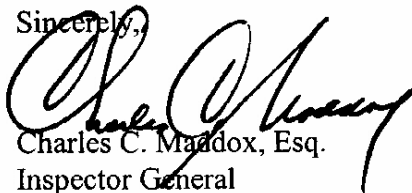
Dear Mr. Abadie and Ms. Peck:

Enclosed is our final report summarizing the results of the District of Columbia (D.C.) Office of the Inspector General (OIG) Audit of the Use of Unauthorized Software at the Office of Contracting and Procurement (OCP). This report is in response to a request by the Director of OCP, that the OIG investigate an OCP employee found to have hacking software installed on his government assigned personal computers. The report was issued in draft as a Management Alert Report (MAR) 02-A-02. Agency comments to the MAR are incorporated in this final report.

We directed two recommendations to OCP and one recommendation to the Office of the Chief Technology Officer (OCTO). OCP concurred with Recommendation 1 and the planned actions are responsive. OCP did not respond to Recommendation 2. We request that OCP provide comments on actions taken or planned in response to Recommendation 2 within 10 days of the receipt of this report. OCTO concurred with the recommendations and has taken corrective actions to correct the deficiencies noted in this report.

We appreciate the cooperation and courtesies extended to our staff during the audit. If you have any questions, please feel free to call me at (202) 727-2540, or William J. DiVello, Assistant Inspector General for Audits, at (202) 727-2540.

Sincerely,



Charles C. Maddox, Esq.
Inspector General

CM/gs

Enclosure

DISTRIBUTION:

The Honorable Anthony A. Williams, Mayor, District of Columbia (1 copy)
Mr. Kelvin J. Robinson, Chief of Staff, Office of the Mayor (1 copy)
Mr. John A. Koskinen, Deputy Mayor and City Administrator (1 copy)
Mr. Tony Bullock, Director, Office of Communications (1 copy)
The Honorable Linda W. Cropp, Chairman, Council of the District of Columbia (1 copy)
Ms. Phyllis Jones, Secretary to the Council (13 copies)
The Honorable Vincent B. Orange, Sr., Chairperson, Committee on Government Operations,
Council of the District of Columbia (1 copy)
Dr. Natwar M. Gandhi, Chief Financial Officer (4 copies)
Ms. Deborah K. Nichols, D.C. Auditor (1 copy)
Mr. Jeffrey C. Steinhoff, Managing Director, GAO (1 copy)
Ms. Jeanette M. Franzel, Acting Director, IRS Financial Management GAO (1 copy)
The Honorable Eleanor Holmes Norton, D.C. Delegate, House of Representatives (1 copy)
Mr. Jon Bouker, Office of the Honorable Eleanor Holmes Norton (1 copy)
The Honorable Joe Knollenberg, Chairman, House Subcommittee on D.C. Appropriations
(1 copy)
Mr. Jeff Onizuk, Legislative Director, House Subcommittee on D.C. Appropriations (1 copy)
Mr. Migo Miconi, Staff Director, House Subcommittee on D.C. Appropriations (1 copy)
The Honorable Chaka Fattah, House Committee on D. C. Appropriations (1 copy)
Mr. Tom Forhan, Minority Staff Director, Office of the Honorable Chaka Fattah (1 copy)
The Honorable Connie Morella, Chairman, House Subcommittee on D.C. Government Reform
(1 copy)
Mr. Russell Smith, Staff Director, House Subcommittee on D.C. Government Reform (1 copy)
Mr. Mason Alinger, Professional Staff Member, Senate Subcommittee on D.C. Government
Oversight (1 copy)
The Honorable Richard Durbin, Chairman, Senate Subcommittee on D.C. Government Oversight
(1 copy)
Ms. Marianne Upton, Staff Director, Senate Subcommittee on D.C. Government Oversight
(1 copy)
The Honorable Mary Landrieu, Chairman, Senate Subcommittee on D.C. Appropriations
(1 copy)
Ms. Kate Eltrich, Staff Director, Senate Subcommittee on D.C. Appropriations (1 copy)
Mr. Stan Skocki, Legislative Assistant, Senate Subcommittee on D.C. Appropriations (1 copy)
Mr. Charles Kieffer, Clerk, Senate Subcommittee on D.C. Appropriations (1 copy)

**AUDIT OF THE USE OF UNAUTHORIZED SOFTWARE AT THE
OFFICE OF CONTRACT AND PROCUREMENT**

TABLE OF CONTENTS

	<u>PAGE</u>
EXECUTIVE DIGEST.....	1
INTRODUCTION.....	4
BACKGROUND	4
OBJECTIVES, SCOPE, AND METHODOLOGY	4
FINDING AND RECOMMENDATIONS.....	6
FINDING: INADEQUATE CONTROLS OVER END-USER COMPUTING	6
EXHIBITS	13
EXHIBIT 1: OFFICE OF CONTRACTING AND PROCUREMENT’S RESPONSES 	13
EXHIBIT 2: OFFICE OF THE CHIEF TECHNOLOGY OFFICER’S RESPONSES. 	19

EXECUTIVE DIGEST

OVERVIEW

This audit was conducted in response to a request by the Director, OCP, that the Office of the Inspector General (OIG) investigate an OCP employee found to have hacking software installed on his government assigned personal computers (PCs) and to advise OCP of possible courses of action.¹ Based on concerns expressed by OCP, the Inspector General made a decision that an audit inquiry would be more appropriate initially, and if the audit inquiry revealed conduct with criminal implications, an investigation of the matter would ensue.

The report was issued in draft as Management Alert Report (MAR) 02-A-02; agency comments to the MAR are incorporated in this final report in Exhibits 1 and 2.

CONCLUSION

Our review confirmed that an OCP computer specialist had installed and operated LOPHT Crack (software that could be used for hacking) on two OCP PCs.² The computer specialist's installation and use of the software went undetected by OCP because, in the absence of District-wide end-user computing guidelines, OCP did not establish adequate internal controls³ over its end-user computing.⁴

We are unable to conclude with certainty that the computer specialist utilized the LOPHT Crack software to compromise the OCP local area network (LAN). However, based on our review, we question the computer specialist's motives for: (1) installing and utilizing LOPHT Crack; (2) possessing passwords belonging to other D.C. Fire and Emergency Medical Services (DCFEMS) Management Information System (MIS) employees; (3) possessing the DCFEMS configuration settings required to logon to the DCFEMS LAN; (4) installing and utilizing Novell Client⁵ when OCP does not need the Novell Client for its computer operations; (5) possessing Outlook⁶ address files and personal e-mail files named after the current OCP Director; (6) utilizing another OCP employee's PC after his assigned PCs were confiscated; and (7) refusing to provide his PC and OCP local area network logon password to OCP management and the OIG.

¹ Hacking, in this instance, refers to gaining unauthorized access to computer systems.

² LOPHT Crack is software designed primarily to capture passwords for users on a local machine or to ferret out passwords and login information over a network. A 30-day trial version can be downloaded from the Internet.

³ Internal controls are policies, procedures, practices, and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.

⁴ End-user computing occurs whenever the user has the tools to generate and manipulate information.

⁵ Novell Client is workstation software that allows the Novell operating system to interface with the Windows desktop environment.

⁶ Outlook is a communication and messaging software and two of its basic features are e-mail and task scheduling.

EXECUTIVE DIGEST

We determined that OCP could have prevented or detected the installation of LOHPT Crack and its use to obtain passwords earlier if District-wide end-user computing guidelines and procedures were in effect. Such policies and procedures would have: (1) prohibited the installation of potentially harmful software on District-owned PCs, and (2) required agencies to actively monitor District-owned PCs for such software. In the absence of District guidelines, OCP should have developed its own end-user computing guidelines. Through discussions with OCTO and information technology (IT) representatives of District agencies, we determined that there is no District-wide policy on this issue and the majority of District agencies have not established their own policies and procedures governing the following areas for end-user computing environments: (1) personal and ethical responsibility; (2) physical security; (3) privacy of electronic communication; and (4) acquisition, implementation, and use of third-party products and services.

As a result, the risk exists that OCP, in this instance, cannot consistently hold employees accountable for equipment and software entrusted to their care or prevent inappropriate PC usage without end-user computing policies and procedures that are consistent with the District's security and internal control framework. End-user computing policies and procedures would provide internal controls and a basis to address inappropriate behavior and to create an awareness program that would foster effective internal controls.

CORRECTIVE ACTIONS

We directed two recommendations to OCP and one recommendation to OCTO that we believe are necessary to correct the deficiencies noted in this report. The recommendations, in part, center on:

1. OCP developing policies and procedures over its end-user computing;
2. OCP taking a personnel action, if deemed appropriate for the circumstances, in accordance with the District of Columbia Personnel Manual, for misuse of government equipment and resources; and
3. OCTO developing policies and procedures over the District's end-user computing environment.

MANAGEMENT COMMENTS

OCP did not indicate whether they concurred or non-concurred with Recommendation 1. However, OCP provided us with an interim Information Technology Security Policy dated December 10, 2001, and stated that they would implement more specific policies governing end-user computing by the 3rd quarter, FY02. OCP did not respond to Recommendation 2.

EXECUTIVE DIGEST

OCTO concurred with Recommendation 3. OCTO stated that they have implemented an Information Technology Security Program that fully covers the issues provided in Recommendation 3. OCTO stated that it is their goal to centralize the policies and procedures and the management of the policies, procedures, and controls.

OIG RESPONSES

OIG believes that OCP's response to Recommendation 1 is adequate and should assist in providing guidance to OCP employees on acceptable usage of computer resources.

OCP did not respond to Recommendation 2. OIG requests that OCP provide comments in response to Recommendation 2 within 10 days after receipt of this report.

OIG believes that OCTO's responses to Recommendation 3 are adequate and should assist District agencies in providing standards and guidance to District employees on acceptable usage of District IT and computer resources.

INTRODUCTION

BACKGROUND

On August 16, 2001, the OCP network services manager received a call from an OCTO network engineer who was monitoring network traffic over the D.C. wide area network (DCWAN).⁷ The OCTO network engineer informed the OCP network services manager that a PC assigned to OCP was emitting an unusually high volume of traffic over the DCWAN. In an effort to determine why the PC was emitting such a high volume of traffic, OCTO dispatched a network engineer to OCP. After consultation with the OCTO network engineer, OCP determined that the PC emitting the unusually high volume of traffic was assigned to the computer specialist. The contractor performing LAN administration services for OCP, in the presence of the OCTO network engineer, had the computer specialist log onto his assigned PC and the OCP network in an attempt to determine what was causing the high volume of network traffic. The OCTO engineer determined that the computer specialist's PC was infected with the CODE RED Worm, which would cause the PC to emit an unusually high volume traffic over the network.⁸

The OCTO network engineer also observed that LOPHT Crack was installed on one of the PCs assigned to the computer specialist. The OCTO network engineer informed his immediate superior, the OCTO Director of IT Security. The OCTO Director of IT Security contacted the OCP Director to inform him that an OCP employee had LOPHT Crack installed on his assigned PC. Subsequently, OCP confiscated two PCs that were assigned to the computer specialist and restricted his building access to coincide with his tour of duty.

As a result of the OCP Director's discussion with OCTO personnel, the OCP Director contacted the OIG to request an investigation of this matter.

OBJECTIVES, SCOPE, AND METHODOLOGY

Based on concerns expressed by OCP, the Inspector General made a decision that an audit inquiry would be more appropriate initially, and if the audit inquiry revealed conduct with criminal implications, an investigation of the matter would ensue.

The objectives of our audit was to determine if: (1) the computer specialist had installed and used unauthorized software on a government PC; (2) the computer specialist had used the unauthorized software to compromise District IT resources; and (3) adequate internal controls had been established over OCP's end-user environment.

⁷ Network traffic includes signals sent from local area network (LAN)/wide area network (WAN) workstations/servers to other workstations/servers throughout the network.

⁸ The CODE RED Worm is a malicious code transmitted over the Internet that causes data flow in unprotected web servers to exceed its data storage areas (buffer-overflow).

INTRODUCTION

Our review was limited to a review of software, hardware, files, and folders contained on two of the computer specialist's assigned government computers.

We accomplished our audit objectives by: (1) conducting interviews with responsible OCTO and OCP management, and other involved personnel; (2) inspecting and inventorying software, hardware, files and folders on the two PCs assigned to the computer specialist; and (3) reviewing other documentation as it became necessary.

Our audit was conducted in accordance with generally accepted government auditing standards.

FINDING AND RECOMMENDATIONS

FINDING: INADEQUATE CONTROLS OVER END-USER COMPUTING

SYNOPSIS

Our review confirmed that the computer specialist had: (1) installed and operated LOPHT Crack on two OCP PCs; (2) installed Novell Client when the OCP computing environment does not require it; and (3) stored questionable documents and e-mail files. We also noted questionable behavior surrounding the computer specialist's usage of another OCP employee's assigned PC and the computer specialist's refusal to provide OCP and OIG management with his assigned PC and OCP local area network logon password.

These conditions occurred and went undetected by OCP because, in the absence of District-wide end-user computing guidelines, OCP did not establish adequate internal controls over its end-user computing. Additionally, OCTO has not implemented District-wide end-user computing guidelines. As a result, the computer specialist was able to install and execute software which would allow him to capture other user's passwords and install and utilize software that was not approved by OCP, apparently without having violated any policy to the contrary.

AUDIT RESULTS

LOPHT Crack - The computer specialist informed us that the former OCP Director tasked him with evaluating OCP's automated procurement system and an e-mail calendar scheduling software, and that he had installed LOPHT Crack on both of his OCP-assigned PCs to assist in this process. The OCP network services manager also informed us that the computer specialist was tasked by the former OCP Director to: (1) evaluate an e-mail calendar scheduling software; (2) assist in developing an IT strategic plan; and (3) evaluate hardware and software prior to its acquisition.

The OCP computer specialist provided us with two memoranda, dated August 15, 2000, and September 18, 2000, to support his assertion that the former OCP Director assigned him evaluating responsibilities. Neither of the memoranda granted explicit permission nor implied that the computer specialist should install and use LOPHT Crack on OCP-assigned PCs. One memorandum contained recommendations from the computer specialist to the former OCP Director suggesting the purchase and evaluation of software designed to capture and recover passwords. However, the computer specialist could not provide us with any documentation indicating whether the former OCP Director agreed with or accepted the recommendations, nor could the computer specialist provide us with documentation of the results of any tests and evaluations performed.

The computer specialist also told us that he did not inform the current OCP Director, the OCP network services manager (his immediate supervisor), or any of the OCP IT staff that he intended to run LOPHT Crack on OCP PCs or against the OCP network. He further stated

FINDING AND RECOMMENDATIONS

that he was unaware of any OCTO, OCP, or District policy forbidding the installation and use of LOPHT Crack.

In order to install LOPHT Crack, the user must have administrator rights to the PC on which the software will be installed.⁹ The OCP network services manager informed us that the computer specialist did not have administrator rights to the OCP LAN, and the computer specialist confirmed that he did not have administrator rights to the OCP LAN. However, we discovered that the computer specialist did have administrator rights to both his OCP-assigned PCs, thereby enabling him to install LOPHT Crack. After executing LOPHT Crack, the computer specialist could utilize the captured logon user names and passwords to assign himself administrator rights to the OCP LAN. With administrator rights, the computer specialist would have had unlimited access to applications and confidential files on the OCP LAN. However, we did not find any logs or data indicating that the computer specialist obtained OCP user accounts and passwords. Instead we found LOPHT Crack logs that contained the user account names and passwords for DCFEMS' IT personnel and contractors working with the DCFEMS MIS division on both of the computer specialist's PCs.

Prior to his employment with OCP, the computer specialist was the former DCFEMS MIS Director. The computer specialist left the employ of DCFEMS in July 2000. We determined that the LOPHT Crack logs were created in October 2000, and that one of the DCFEMS user passwords contained in the log was active until we notified DCFEMS in October 2001 of the need to change passwords. We also determined that the DCFEMS employee, whose password was active, had administrator rights. Consequently, the computer specialist could have used the DCFEMS employee's name and password, with the corresponding administrator rights, to access the DCFEMS LAN and take full control of the LAN resources.

The current DCFEMS MIS Director informed us that the computer specialist's access account was closed and the systems administrator password changed after the computer specialist left DCFEMS. However, DCFEMS IT personnel informed us that the last access to the DCFEMS LAN using the computer specialist's user name was on October 19, 2000, **three months** after he left DCFEMS. In addition, we noticed that the name of another former DCFEMS MIS Director, who left in October 2000, appeared in the Novell Client login user name box on one of the computer specialist's OCP-assigned PCs, and that someone using this former DCFEMS MIS Director's user name last accessed the DCFEMS LAN on January 27, 2001.

The computer specialist informed us that on several occasions, both OCTO and DCFEMS personnel requested that he access the DCFEMS LAN to unlock accounts and retrieve information. However, the current DCFEMS MIS Director informed us that DCFEMS has its own IT staff and LAN administrators and that the computer specialist had no authority or responsibility requiring that he access the DCFEMS LAN after his departure. We could not determine conclusively that the computer specialist utilized LOPHT Crack to compromise the

⁹ Administrator rights are granted to the person responsible for the operation of the network and allow the administrator, or designated persons, to have full control over the operating system and network resources.

FINDING AND RECOMMENDATIONS

OCP LAN and gain access to sensitive files and folders or that the computer specialist accessed the DCFEMS LAN.

Novell Client - In addition to LOPHT Crack, the computer specialist also had Novell Client installed on both of his OCP-assigned PCs. The contractors responsible for administering OCP's LAN informed us that OCP employees do not need Novell Client installed on OCP PCs because OCP uses Windows NT and Novell Client is used to access Novell Servers.¹⁰ The computer specialist informed us that he installed Novell Client because of personal preference.

The DCFEMS MIS Director told us that DCFEMS uses the Novell operating system for its servers. The computer specialist had the DCFEMS Tree¹¹, DCFEMS Context¹², and DCFEMS Server's Internet protocol (IP) address¹³ on both PCs Novell Client logons. Accordingly, the computer specialist could logon to the DCFEMS servers with this configuration using the user names and passwords he obtained from executing LOPHT Crack.

In addition, we found that a directory on one of the computer specialist's assigned PCs contained a mapping¹⁴ to a DCFEMS server's IP address.¹⁵ In order to map to a server, the user must have an account on the destination server. The computer specialist would not have been able to map to the DCFEMS server without first having an account and password to the DCFEMS server. The computer specialist informed us that the reason he had DCFEMS configurations on his OCP-assigned PCs was because he imaged his OCP-assigned PCs from PC configurations he had while at the DCFEMS. However, based on the computer specialist's current employment and position description at OCP, we found no need for the computer specialist to have the DCFEMS server and domain configurations.

Documents and E-mails - We found two Outlook files on one of the computer specialist's OCP assigned PCs named "AbadieJ.Pab" and "AbadieJ.Pst". The Pab extension indicates the file is the address book file for Outlook and the Pst extension is the personal file where e-mails are kept. However, neither of the files contained any addresses or e-mails. The computer specialist informed us the files may have inadvertently gotten on his PC while setting up the OCP Director's calendar software. We also found numerous documents and e-mails regarding work conducted during the computer specialist's employment with DCFEMS, but we were unable to determine conclusively that the computer specialist logged onto DCFEMS's LAN after he left DCFEMS to obtain the documents and e-mails.

¹⁰ A server is a computer or device on a network that manages network resources. For example, a *file server* is a computer and storage device dedicated to storing files.

¹¹ A tree is a hierarchical arrangement that shows the relationship of a grouping of computers (domain) to each other and other network resources.

¹² Context is the position of an object within the Directory tree structure.

¹³ An IP address is a logical 32-bit address that identifies a transmission control protocol (TCP)/IP host.

¹⁴ A mapping is the designation of a path to a particular resource.

¹⁵ An OCTO security representative identified the IP address as one belonging to DCFEMS.

FINDING AND RECOMMENDATIONS

Questionable Behavior - An OCP employee stated that upon arrival at work, August 23, 2001, when attempting to logon to the OCP LAN, she noticed that the computer specialist's user name was in the login user name box on her OCP assigned PC. The computer specialist informed us that he might have used the OCP employee's assigned PC to download a report. This occurred after OCP had confiscated the computer specialist's two OCP assigned PCs.

The OCP LAN administrator provided us with security logs that indicated that someone using the OCP employee's assigned PC and the computer specialist's user name logged on and off of the OCP LAN on August 22, 2001, fourteen times between the 7:14 PM and 10:45 PM. The security logs also indicated that someone using the OCP employee's assigned PC invoked privilege use,¹⁶ object access,¹⁷ and the account manager.¹⁸

The computer specialist informed us that he was confused about the date and times on the event logs. The computer specialist said he did not recall being in OCP during the times in question. We requested from the OCP Security Manager the August 22, 2001, building access logs for the 441 Judiciary Square Building to determine if the computer specialist's building access card had been used to enter the building on the date and times indicated on the security logs. However, OCP was unable to provide us with the building access logs. The OCP security manager informed us that the building facility manager was unable to obtain the building access logs for the requested date. As a result, we were unable to determine if the computer specialist's building access card was used to access the building on the date and times indicated on the security log.

The Network Services Manager informed us that the computer specialist refused to provide his password for logging onto the OCP network and local PC. The Network Services Manager said the computer specialist offered to change his password and then provide it to him. We also requested the computer specialist provide us with the password to the PC containing the Windows 2000 operating system. However, the computer specialist refused and changed the password. The computer specialist said he did not want to provide his password because he uses the same password to logon to other systems and it might compromise his security. After we gained access to the Windows 2000 PC, we observed that the computer specialist had a mapping to a DCFEMS server. As a result of changing the password, we were unable to determine if the computer specialist had access to the DCFEMS server. If the original password had been provided, it could have possibly provided the logon connection to the DCFEMS server.

¹⁶ Event describes both successful and unsuccessful attempts to use privileges. Privileges are a user right which is assigned to a user and that specifies allowable actions on the network. An example of a privilege is the right to shut down a system.

¹⁷ Event describes both successful and unsuccessful accesses to protected objects. Objects are entities such as a file, folder, shared folder, printer, or Active Directory object described by a distinct, named set of attributes.

¹⁸ Event describes high-level changes to the user account database. Account manager is a tool used to manage user accounts and groups. Tool can be used to create new users and groups, add users to groups, remove users from groups, disable user and group accounts, and reset passwords.

FINDING AND RECOMMENDATIONS

The computer specialist's PC with Windows NT was a member of the OCP domain and the PC with Windows 2000 was not. The OCP LAN administrator has control over all PCs within the OCP domain.¹⁹ However, the computer specialist's PC with Windows 2000 was configured as a workgroup and not under the control of the OCP LAN administrator. This configuration would allow the computer specialist to utilize the PC with Windows 2000 to authenticate to the OCP domain through the PC with Windows NT and utilize OCP domain resources without the OCP LAN administrator having control over the PC. Adequate internal controls would provide that the administrator have physical and access control to all PCs within the organization.

RECOMMENDATION 1. We recommend that the Director of the Office of Contracting and Procurement develop interim policies and procedures over end-user computing, pending the completion of actions taken to resolve Recommendation 3 directed to the Office of the Chief Technology Officer. At a minimum, these policies and procedures should cover:

- a) personal and ethical responsibility;
- b) physical security;
- c) privacy of electronic communications;
- d) acquisition, installation, and use of third-party products and services; and
- e) penalties for unauthorized use.

Agency Comments

OCP did not indicate whether they concurred or non-concurred with Recommendation 1. However, OCP provided us with an interim Information Technology Security Policy dated December 10, 2001. The policy covers: (1) personal and ethical responsibility; (2) physical security; (3) privacy of electronic communications; (4) acquisition, installation and use of third-party products and services; and (5) penalties for unauthorized use. OCP further stated that it plans to issue specific written policies and procedures covering (1) desktop computing, (2) remote access, (3) network usage, and (3) virus protection policy and procedure. OCP stated that this policy should be implemented by the end of the 3rd quarter, FY02.

OIG Response

OCP's response to Recommendation 1 is adequate. When fully implemented, the policy should assist OCP in providing guidance to OCP employees on acceptable usage of OCP computer resources.

¹⁹ In this situation, control means the ability of the OCP LAN administrator to access the PCs through administrative functions.

FINDING AND RECOMMENDATIONS

RECOMMENDATION 2. We recommend that the Director of the Office of Contracting and Procurement take personnel action, if deemed appropriate for the circumstances, in accordance with the District of Columbia Personnel Manual, for misuse of government equipment and resources.

Agency Comments

The OCP did not provide comments in response to Recommendation 2.

OIG Response

OIG requests that OCP provide comments on corrective action planned or taken in response to Recommendation 2 and provide comments within 10 days after receipt of this report.

RECOMMENDATION 3. We recommend that the Office of the Chief Technology Officer develop District-wide policies and procedures over end-user computing. At a minimum, these policies and procedures should cover:

- a) personal and ethical responsibility;
- b) physical security;
- c) privacy of electronic communications;
- d) acquisition, installation, and use of third-party products and services; and
- e) penalties for unauthorized use.

Agency Comments

OCTO concurred with Recommendation 3. OCTO stated that they have implemented an Information Technology Security Program that fully covers the issues provided in our Recommendation 3. OCTO stated that it is their goal to centralize the policies and procedures and the management of the policies, procedures, and controls.

OIG Response

The OIG believes that OCTO's response to Recommendation 3 is adequate and should assist District agencies in providing standards and guidance to District employees on acceptable usage of District IT and computer resources.

FINDING AND RECOMMENDATIONS

Additional Comments

OCTO and OCP should consider incorporating in their end-user policies and procedures provisions for ensuring that the administrator has the authority, responsibility, and capability for controlling all computer resources operating on or through an agency's computer network. The provisions for control should include, at a minimum, the administrator's authority for physical and logical access to all the agency computer resources; and authority, responsibility, and capability for identification and inventory of all hardware and software operating on the agency's computer network.

EXHIBITS

EXHIBIT 1: OFFICE OF CONTRACTING AND PROCUREMENT'S RESPONSES

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of Contracting and Procurement

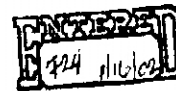
Director

★ ★ ★
[REDACTED]
[REDACTED]

2002 JAN 16 PM 2:

January 15, 2002

Charles C. Maddox, Esq.
Inspector General
717 14th Street, NW
5th Floor
Washington, DC 20005




Dear Mr. Maddox:

The attached Office of Contracting and Procurement interim "Information Technology Security Policy" is in response to your Management Alert Report (MAR 02-A-02), dated 10 December 2001. This interim policy covers: a. personal and ethical responsibility, b. physical security, c. privacy of electronic communications, d. acquisition, installation and use of third-party products and services, e. penalties for unauthorized use.

The Office of Contracting and Procurement also has plans to issue specific written policies and procedures on: a. desktop computing, b. remote access, c. network usage, and d. virus protection policy and procedure. These policies will be staffed and implemented by the end of the 3rd quarter, FY02.

If you have questions or need additional information relative to this response, please call [REDACTED] Manager for IT Services or me at (202) 727-0252.

Sincerely,


Jacques Abadie III, CPCM
Chief Procurement Officer

cc: John A. Koskinen, Deputy Mayor and City Administrator
Suzanne Peck, Chief Technology Officer
[REDACTED] General Counsel
[REDACTED] Assistant Director
[REDACTED] Assistant Director
[REDACTED] Manager for IT Services

441 4th Street N.W., Suite 800 South, Washington, D.C. 20001
(202) 727-0252 Fax: (202) 724-5673

EXHIBITS

EXHIBIT: 1 OFFICE OF CONTRACTING AND PROCUREMENT'S RESPONSES



INFORMATION TECHNOLOGY SECURITY POLICY

January 2002

EXHIBITS

EXHIBIT: 1 OFFICE OF CONTRACTING AND PROCUREMENT'S RESPONSES

Information Technology (IT) Security Policy Office of Contracting and Procurement

All Office of Contracting and Procurement (OCP) personnel, contractors and guests are expected to abide by all OCP IT policies and guidelines. All employees are responsible for protecting OCP information from unauthorized access, modification, duplication, destruction, or disclosure. As employees of OCP, we share a common responsibility to protect OCP's interest. If you have a concern about potential violations of this policy contact your supervisor.

The computer and electronic communications systems maintained by OCP for business are the property of OCP, unless otherwise specified. Employees should not have an expectation of privacy in anything they create, store, send, or receive on those systems. All usage is subject to audit or review by management without additional notification to the individual employee. Full cooperation of all employees is required during any such audits or review.

It is expected that during work hours the computer, its systems, and the Internet will be used for business purposes. Incidental personal use is restricted to non-work hours only. This is before and after normal working hours and during lunch.

Employees who violate these policies may be subject to corrective action, which may include termination, and may be held personally responsible for any and all damages or claims.

Acquisition of Hardware and Software

All hardware and software acquired for use on OCP computer systems will be obtained through established procedures. This includes purchase order, purchase card, petty cash, lease, rental and trial use hardware and software. Contact your supervisor for the approval process.

Copyright and Software License Compliance

OCP strives to respect all computer software copyrights and to adhere to the terms of all software licenses to which OCP is a party. Unless OCP or its employees are expressly authorized to do so by written agreement with the owner/author, employees are strictly prohibited from duplicating any licensed software or related documentation (except for backup and archival purposes) for use either on OCP's premises or elsewhere.

Assume that all information retrieved from the Internet is copyrighted information. Copying, sending, or receiving trademarked, copyrighted materials, trade secrets, proprietary information, or other similarly sensitive materials such as documents, graphics, video clips, audio clips, or third-party software without the express written permission of the owner or the proper license is prohibited.

Unauthorized use or duplication of software may subject individual employees and OCP to civil and/or criminal penalties, including fines or imprisonment, under the United States Copyright Act or other District or federal laws.

Likewise, employees are not permitted to install software personally purchased onto OCP computers. OCP reserves the right to inventory all software on each OCP-owned computer or laptop.

EXHIBITS

EXHIBIT: 1 OFFICE OF CONTRACTING AND PROCUREMENT'S RESPONSES

Electronic Communication (E-mail, Facsimile, Voice)

Electronic communication capabilities are provided to employees as a way to facilitate communication and their use is intended to satisfy a business need. All electronic messages created, sent, or received by OCP employees through the use of OCP's electronic systems are the property of OCP. Incidental personal use of electronic communication systems may be allowed as defined by your supervisor or manager, but such use must comply with all policies and guidelines. Examples of forms of electronic communications include E-mail, facsimiles and voice communication systems (telephone usage).

Any incoming personal E-mail with attachments must be scanned with virus protection software prior to opening. If a virus is detected, the E-mail message will be deleted and must not be forwarded. Attachments transport viruses.

Employees have no right of privacy in any electronic communication. The OCP reserves the right to access, monitor, audit and/or disclose all active or archived messages sent electronically. Electronic messages are subject to review by management without additional notification to the individual employee. Most electronic communication systems create a record that can be saved, replayed, and shared with others and should always be considered a non-private communication method. Employees should be aware that OCP does a full back-up of all daily network activity every day at 11:00 PM. Even when an electronic message has been deleted, a record or back-up copy remains and can be accessible by OCP.

Employees should draft electronic messages with the same thought and concern as they would give to written correspondence. Sending or attempting to send disruptive, discriminatory, harassing, offensive, abusive, obscene, defamatory information or statements, and/or threatening electronic communication to any other user is expressly prohibited.

The OCP Logos

OCP controls its logos and trademarks (known as "marks" and typically designated by a TM, ® or SM) in order to protect their integrity in the marketplace and registered status.

The OCP-owned marks are to be used for authorized OCP business only. Misuse or unauthorized use of OCP marks is strictly prohibited. The marks or logos can only be used as they appear in the file format and cannot be altered or modified.

Internet Use

Employees may be provided with access to the Internet when there is a business need to do so. Incidental personal use of the Internet may be allowed as defined by your supervisor or manager, but such use must comply with all OCP policies and guidelines. The access, display, storage, or transmission of pornographic materials or other such information whose political, sexual, racial, religious, or other content could be considered offensive by employees, clients, or third parties is expressly prohibited. If this privilege is abused, the ability to access the Internet may be removed, and further corrective action may result.

Transmitting sensitive OCP information via the Internet is restricted including, employee information, client lists, claims information, purchase card information, and unauthorized transfer of software or vendor information.

EXHIBITS

EXHIBIT: 1 OFFICE OF CONTRACTING AND PROCUREMENT'S RESPONSES

All Internet usage including downloading information is monitored by the Office of the Chief Technology Officer (OCTO) and can be monitored by OCP if required. An electronic log is automatically created for each individual identifying the sites visited and time spent on the Internet. This log is subject to review by management without additional notification to the individual employee.

Mobile Computing

All OCP policies apply to the use of computing resources outside the office. It is the employee's responsibility to use reasonable precautions to protect the asset from theft or unauthorized access

Only approved hardware and software is allowed for remotely connecting to the DCWAN network. Computer hardware and software provided by OCP for remote access purposes must not be altered or enhanced in any way. Such hardware must be returned when the employee terminates employment with OCP or transfers to a different agency.

Remote access is permitted for employees with a business need, with the Chief Procurement Officer's approval.

Computer security - Employees are responsible for respecting the privacy of others. Employees may not alter or copy a file belonging to another employee without first obtaining permission from the owner of the file. Monitoring or accessing another employee's information may not be done without business reasons and authorization. The capability to access a file belonging to another employee does not imply permission to read, alter, or copy that file.

Employees may not gain or attempt to gain unauthorized access to restricted areas or files on any OCP computer systems including bypassing OCP's data protection measures or uncovering security loopholes. Employees may not alter any software protections or restrictions placed on computer applications, files, or directories.

Responsibility for passwords - Employees are responsible for safeguarding passwords they use to access OCP's computer systems. All activity generated from the employee's ID and passwords are the responsibility of the owner. Employees may not disguise their identity while using the computer systems. Use of passwords to gain access to the computer systems, particular files or messages does not imply that employees should have an expectation of privacy in the material they create or receive on the computer systems.

Supervisors should make efforts to obtain passwords of protected or encrypted documents prior to employee transfer or termination. A terminated employee's individual ID and password shall be eliminated immediately through prompt notification by the terminated employee's supervisor

Allowed use of computer resources - Employees may be permitted access to the computer system to assist them in the performance of their jobs. Incidental and occasional personal use of the computer system may also be permitted, provided that the use does not interfere with the employee's work performance, with any other employee's work performance, or violate any policy or guideline of OCP.

EXHIBITS

EXHIBIT: 1 OFFICE OF CONTRACTING AND PROCUREMENT'S RESPONSES

Use of systems and/or networks in an attempt to gain unauthorized access to remote systems is strictly prohibited. At all times, employees have the responsibility to use computer resources in a professional, ethical, and lawful manner.

Employees should not waste computer resources (e.g. sending mass mailings or chain letters, subscribing to non business-related servers and mailing lists, spending excessive amounts of time on the Internet, playing games, or otherwise creating unnecessary network traffic). Because audio and video files require significant network resources, files of this sort should not be electronically transmitted unless they are business-related.

Employees are not permitted to use computer systems to electronically post or display material that is offensive, libelous, or harassing in nature. Religious or political lobbying is also prohibited.

Personal use of the computer system is a privilege that may be revoked at any time.

Use of Technology Assets

Employees will not be permitted to bring non-OCP owned computer hardware and attach it to any OCP technology assets. This includes hardware such as printers, scanners, workstations, laptops, digital cameras, and modems. If you have any questions regarding appropriate use of a particular technology not specifically identified in this policy, please contact the Help Desk at 724-4735.

Virus Checking

A computer virus is defined as any computer software program that causes or influences either hardware or software to operate in a manner contrary to the intentions or in a manner unapproved by the original owner/user of said software or hardware. Viruses may be intentionally or inadvertently introduced into a computer and then spread or self-replicated to other systems. Examples of how viruses can be spread are the use of diskettes/CD-ROMs acquired from external sources, opening e-mail from unknown authors, or downloading files from Internet sites.

It is the responsibility of each employee to use reasonable care to prevent the introduction of viruses into their systems and the possible further destruction of other systems. If you receive notification that your personal computer has a virus, contact the Help Desk immediately for assistance in cleaning or purging the infected file.

All OCP employees are expected to ensure that all OCP- and OCP employee-owned computers, electronic files, and electronic media used to conduct OCP business are protected from computer viruses. Employees are not permitted to override the virus detection software

EXHIBITS

EXHIBIT 2: OFFICE OF THE CHIEF TECHNOLOGY OFFICER'S RESPONSES

GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE CHIEF TECHNOLOGY OFFICER



2002 JAN 10 AM 10:35

January 7, 2002

Charles C. Maddox, Esq.
Inspector General
Government of the District of Columbia
717 14th Street, NW
Washington, DC 20005



Dear Mr. Maddox:

This letter is intended to provide comments and responses to the recommendations found in the Management Alert Report (MAR 02-A-02).

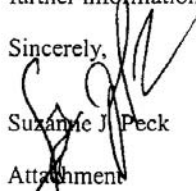
We'd like to address the comments and recommendations on page six of the MAR, specifically directed at the development of District-wide policies and procedures over end-user computing. The report asserts that the Office of the Chief Technology Officer should develop District-wide policies and procedures that cover at a minimum:

- a) personnel and ethical responsibility;
- b) physical security;
- c) privacy of electronic communications;
- d) acquisition, installation, and use of third-party products and services; and
- e) penalties for unauthorized use.

OCTO agrees. We've implemented an Information Technology Security Program which fully covers all the above policies and procedures. The mission of this program is not only to establish centralized policies and procedures but to centralize the management of these policies, procedures and controls. Specific policies and procedures addressing the identified end-user computing issues have been put into effect. They are represented in the attached matrix.

Thank you for the opportunity to comment on this report. Should you have any questions or require further information, please contact me directly

Sincerely,


Suzanne J. Peck

Attachment

cc: John Koskinen
Jacques Abadie

441 4th Street, N.W., Suite 930 South, Washington, DC 20001 Tel: (202) 727-2277 Fax: (202) 727-6857 Email: octo@dc.gov

EXHIBITS

EXHIBIT 2: OFFICE OF THE CHIEF TECHNOLOGY OFFICER'S RESPONSES

Policy Name	Policy Area				
	Personal and Ethical Responsibility	Physical Security	Privacy of Electronic Communications	Acquisition, Installation, and Use of Third-Party Products and Services	Penalties For Unauthorized Use
Information Security Policy	<ul style="list-style-type: none"> States responsibility to maintain the confidentiality, integrity and availability of government information 		<ul style="list-style-type: none"> Confidential data must be protected from unauthorized disclosure No right to personal privacy 		<ul style="list-style-type: none"> States that a violation . . . shall be brought to the attention of agency directors for appropriate action and could result in termination of employment
Information Security Audit Trail Monitoring and Reporting Standard	<ul style="list-style-type: none"> Defined responsibilities apply to all agency employees, contractors and volunteers 	<ul style="list-style-type: none"> Sets forth physical security controls for audit trail files (e.g., backups, access, etc.) 			<ul style="list-style-type: none"> Requires incident escalation to OCTO and IG
Data Sensitivity Standard (Draft)	<ul style="list-style-type: none"> Defines responsibilities for categorizing data 	<ul style="list-style-type: none"> Specifies labeling and handling guidelines for media containing sensitive data 	<ul style="list-style-type: none"> Prohibits unauthorized disclosure of sensitive information 		
Procedures for Handling Computer Security Incidents (Draft)	<ul style="list-style-type: none"> Sets forth standards for addressing computer security incidents 	<ul style="list-style-type: none"> Defines physical controls relative to handling PCs involved in security incidents 			
Desktop Security Standard (Draft)	<ul style="list-style-type: none"> Defines standards for ensuring IT assets are secured 	<ul style="list-style-type: none"> Defines physical controls for protecting confidential data 		<ul style="list-style-type: none"> Prohibits the installation of unauthorized software or hardware Explicitly prohibits use of unauthorized security scanning tools 	<ul style="list-style-type: none"> States that users who illegally access District systems or data may be subject to criminal prosecution under computer crime laws

EXHIBITS

EXHIBIT 2: OFFICE OF THE CHIEF TECHNOLOGY OFFICER'S RESPONSES

Policy Name	Policy Area				
	Personal and Ethical Responsibility	Physical Security	Privacy of Electronic Communications	Acquisition, Installation, and Use of Third-Party Products and Services	Penalties For Unauthorized Use
Network Connectivity Standard	• Sets forth connectivity requirements applicable to all agencies and devices connected to the DC WAN	• Establishes requirements for secure processing areas/locations			• States that violation of prescribed policies, standards and procedures will result in termination of DC WAN services
Physical Security Control Standard (Draft)	• Defined responsibilities apply to all agency employees, contractors and volunteers	• Establishes the minimum level of security controls to ensure physical access is limited to authorized personnel only			
Remote Access Standard (Draft)	• Defined responsibilities apply to all agency employees, contractors and volunteers		• Includes responsibility to ensure confidentiality is maintained	• Requires installation of approved virus protection software	• States that intentional or neglectful violation of any provision of the standard can result in: <ul style="list-style-type: none"> o Revocation remote access o Legal action o Monetary restitution o Disciplinary sanctions
Risk Management Standard (Draft)	• Defined responsibilities apply to all agency employees, contractors and volunteers				

EXHIBITS

EXHIBIT 2: OFFICE OF THE CHIEF TECHNOLOGY OFFICER'S RESPONSES

Policy Name	Policy Area				
	Personal and Ethical Responsibility	Physical Security	Privacy of Electronic Communications	Acquisition, Installation, and Use of Third-Party Products and Services	Penalties For Unauthorized Use
Software Acquisition Standard	<ul style="list-style-type: none"> Lists standards for addressing illegally copied software and license misuse 			<ul style="list-style-type: none"> Contains standards of conduct with respect to software acquisition, copying, transfers and use within the District of Columbia 	<ul style="list-style-type: none"> States that may be a violation of District Security policy, and federal and state law, no specific penalties noted.
Software Management Standard	<ul style="list-style-type: none"> Defines unacceptable software use Contains an Agreement on the use of PC Software, which requires user signature 	<ul style="list-style-type: none"> Sets forth requirement and procedures for periodic, physical software inventory 		<ul style="list-style-type: none"> Defines actions that signify unacceptable software use. 	<ul style="list-style-type: none"> States that employees who make, acquire, or use unauthorized copies of computer software shall be disciplined, which may include termination
User Password Protection Procedure	<ul style="list-style-type: none"> Establishes 12 mandatory user password practices 	<ul style="list-style-type: none"> Includes physical password controls (e.g., no written passwords, etc.) 			<ul style="list-style-type: none"> Agency has responsibility for ensuring compliance
Virus Protection Standard (Draft)	<ul style="list-style-type: none"> Sets forth guidelines for protecting against and/or causing the spread of viruses 	<ul style="list-style-type: none"> Specifies appropriate use of diskettes 		<ul style="list-style-type: none"> Includes prohibitions on the use of externally provided software 	<ul style="list-style-type: none"> States that anyone writing and releasing and/or knowingly proliferating any virus will be subject to immediate termination and held legally accountable for damages
Internet Access and Use Policy	<ul style="list-style-type: none"> Contains principles for use and lists prohibited activities 				<ul style="list-style-type: none"> OCTO refers violations to the affected agencies

EXHIBITS

EXHIBIT 2: OFFICE OF THE CHIEF TECHNOLOGY OFFICER'S RESPONSES

Policy Name	Policy Area				
	Personal and Ethical Responsibility	Physical Security	Privacy of Electronic Communications	Acquisition, Installation, and Use of Third-Party Products and Services	Penalties For Unauthorized Use
Email Use Policy	<ul style="list-style-type: none">• Defines standards for appropriate use of email		<ul style="list-style-type: none">• Email is considered public record – not to be considered private• Sensitive (e.g., confidential) data shall not be transmitted unless appropriately secured		<ul style="list-style-type: none">• Enforcement is an agency responsibility